Cyber Hygiene Program
7 Passi per mitigare un attacco

Alessio L.R. Pennasilico

Andrea Argentin

Verona, Ottobre 2018

Clusit

Clusit
Education

Alessio L.R. Pennasilico aka -=mayhem=-

Practice Leader Information & Cyber Security Advisory @ P4I

Membro del Comitato Direttivo e del Comitato Tecnico Scientifico Clusit Associazione Italiana per la Sicurezza Informatica

Presidente dell'Associazione Informatici Professionisti AIP Associazione Informatici Professionisti ITCS Italian Computer Society

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità Lloyd's Register LRQA

Membro del Comitato di schema kiwa intertek Total Quality. Assured.

Direttore Scientifico della testata CYBERSECURITY360

Andrea Argentin

Andrea Argentin: Pre-Sales Manager in CyberArk. Con un’esperienza di oltre 15 anni nel mercato dell’Information Technology, ha iniziato il suo percorso professionale nell’area sistemistica, specializzandosi poi nel settore della security, in diverse società di consulenza e system integration. Prima di approdare in CyberArk, è stato Security Consultant in Reply, lavorando a stretto contatto con clienti di fascia Enterprise. Nel 2014 in CyberArk assume il ruolo di Sales Engineer, per giungere alla posizione di Pre-Sales Manager. È attualmente responsabile del coordinamento dell’enablement del gruppo di prevendita, oltre ad occuparsi di supporto alle vendite e sviluppo di progetti per clienti Enterprise. È inoltre uno degli evangelist di CyberArk: tiene presentazioni e sessioni dimostrative delle soluzioni e tecnologie del brand, sia presso i clienti sia ad eventi di settore, workshop e conferenze.

Cybercriminals steal $81 million from central bank

BREACH OVERVIEW	
Target	Bangladesh Central Bank
Attacker	Unknown
Motivation	Monetary
Outcome	$81M stolen and unrecovered

May 15, 2015:
Three bank accounts are opened at RCBC

January 29:
SysMon installed on SWIFT-connected systems

February 5 (AM):
Bank's printers go down

Mid-January 2016:
Attackers break into the network

February 4:
Attackers steal credentials of SWIFT users

February 5 (PM):
Fraudulent transactions sent

The End Results

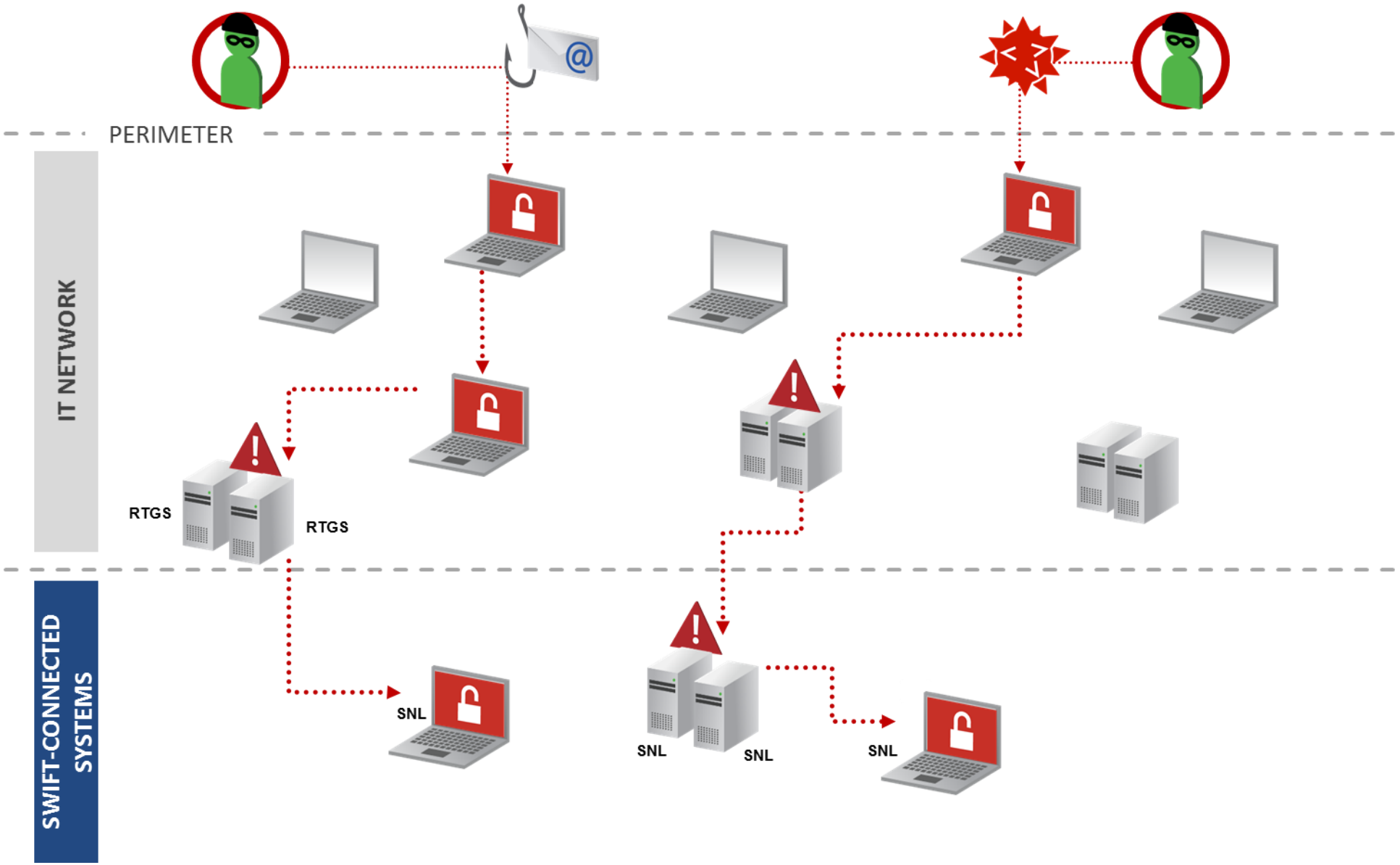
$81 million stolen and unrecovered

Millions laundered through casinos

Central bank governor **resigns**

Security **investigator missing** for six days

The pathway into SWIFTNet starts at the perimeter



The damage could have been far worse

35 ORDERS WORTH **$951 MILLION** WERE SENT

5 ORDERS WORTH $101 MILLION WERE EXECUTED BY THE NY FED

$20 million transferred to Pan Asia Banking Company

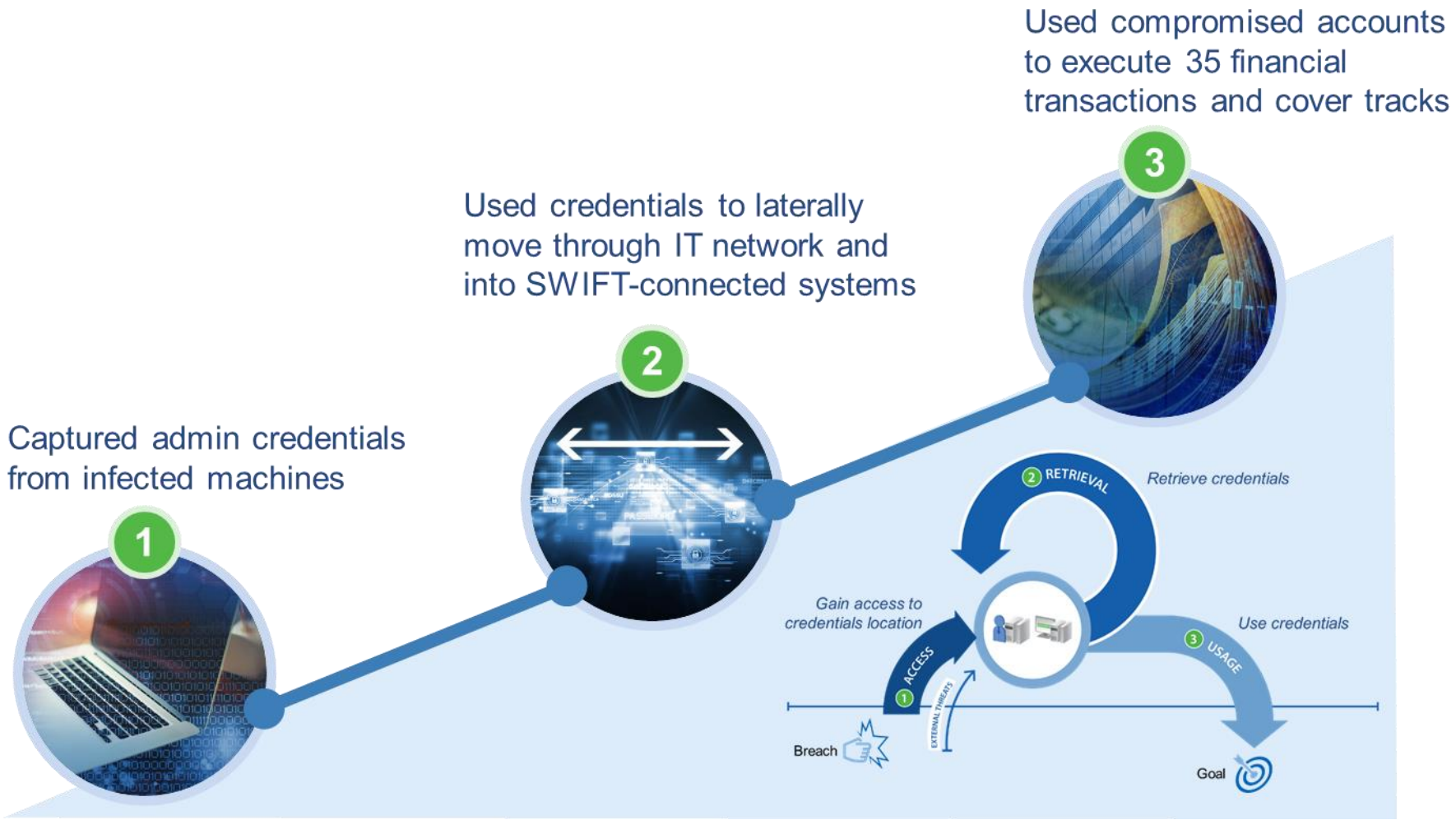
- $20 million stopped en route to "Shalika Fandation"

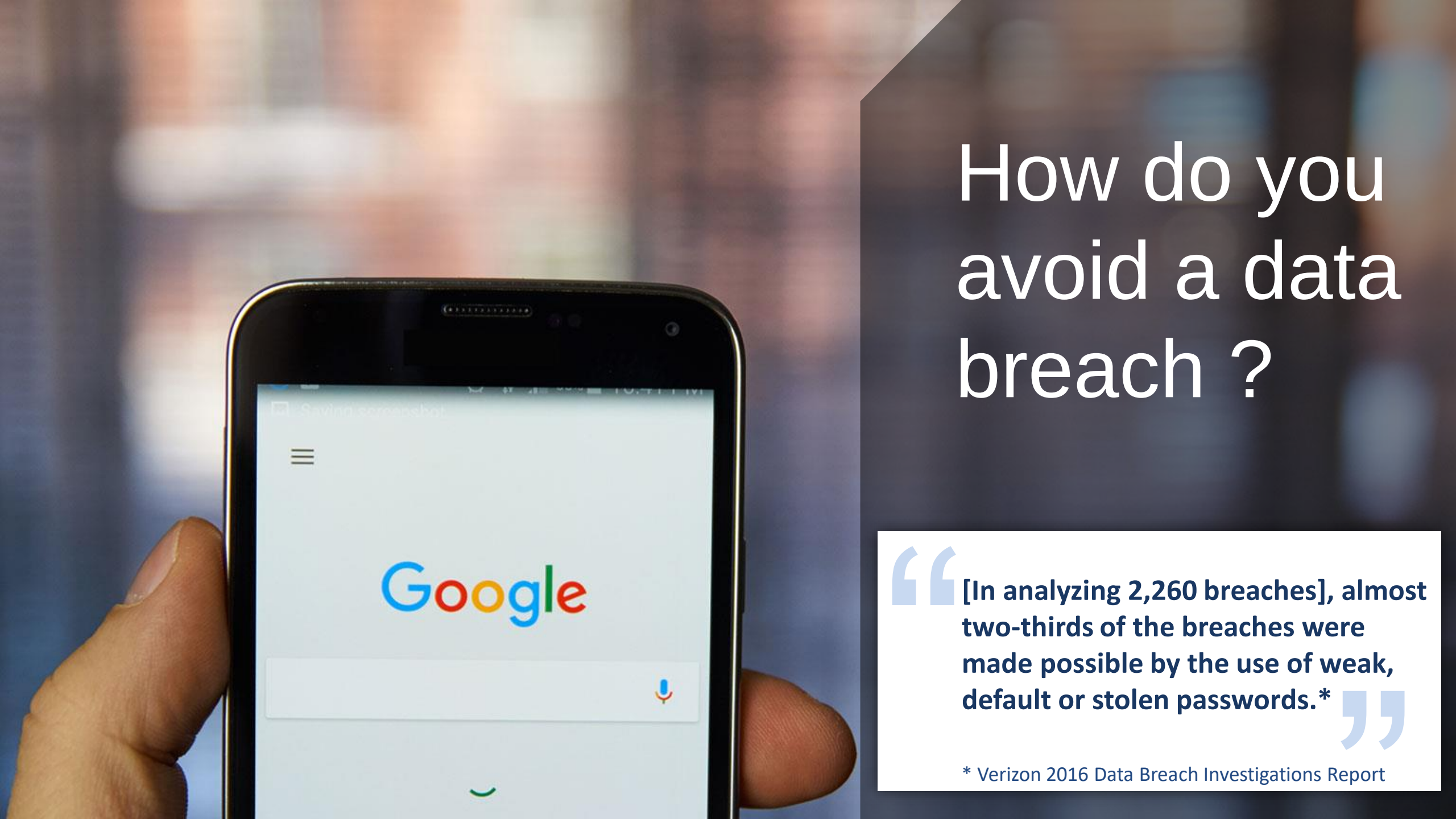
$81 million transferred to RCBC in the Philippines

- $29 million sent to hotel company
- $31 million delivered in cash to a guest of the hotel
- $21 million sent to a leisure company

30 ORDERS WORTH $850 MILLION WERE BLOCKED DUE TO A SUSPICIOUS RECIPIENT

The Role of Privilege in the Bangladesh Bank Heist





How do you avoid a data breach ?

> **[In analyzing 2,260 breaches], almost two-thirds of the breaches were made possible by the use of weak, default or stolen passwords.***

* Verizon 2016 Data Breach Investigations Report

First 3 Steps

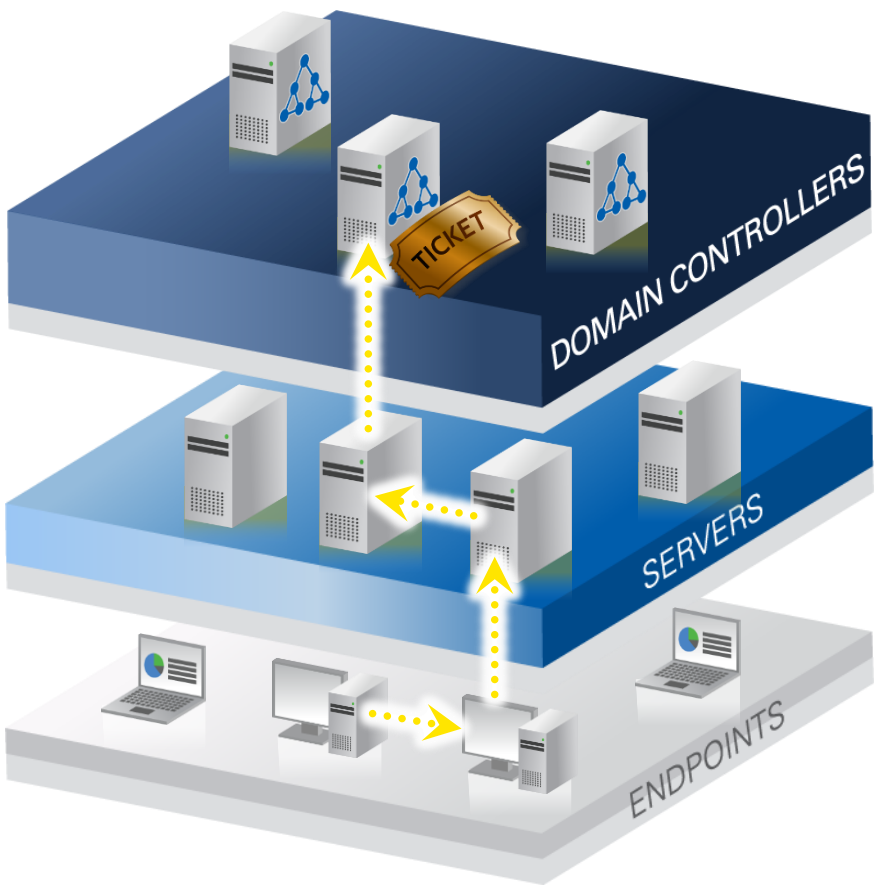
ATTACKER'S MINDSET:

1) Establish persistence in an organization by performing an attack that is not only hard to identify but also so intrusive that the business must rebuild to remove the attacker, e.g., a Kerberos attack such as a Golden ticket

2) Take ownership of an entire technology stack by compromising a single infrastructure account, and use the same credentials on similar assets

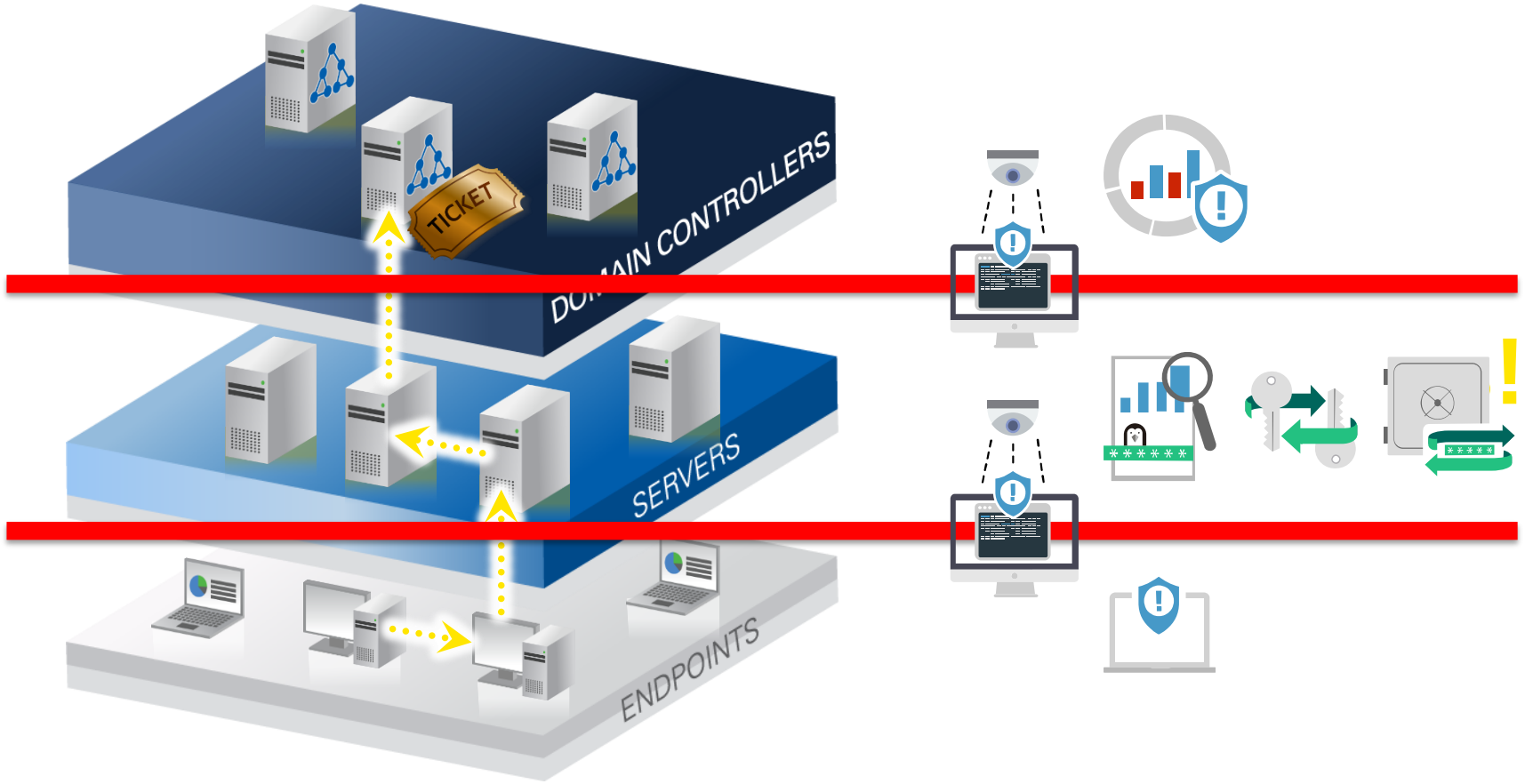
3) Stealing credentials and moving laterally to IT Windows workstation in order to steal elevated permissions.

The Privileged Pathway



10 **Minutes!**

The Privileged Pathway



Key finding:
Attackers exploited vulnerabilities with Windows admin credentials

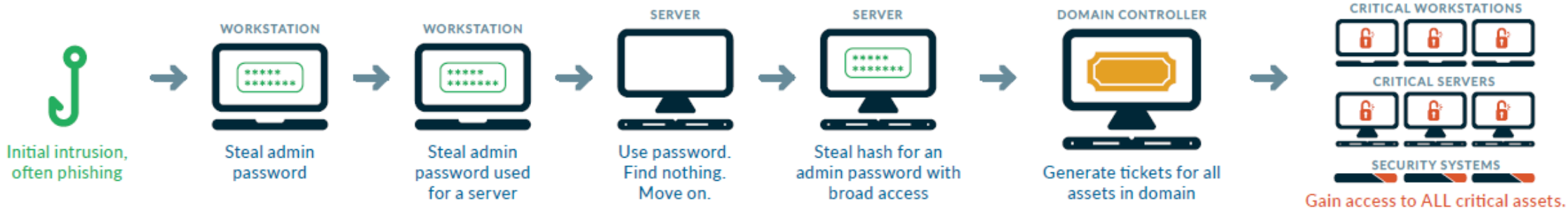
Common practices that make organizations susceptible to attack

- **Providing end users with local admin rights on their workstations**
- **Having IT helpdesk staff use domain admin accounts for troubleshooting**
- **Giving IT admins access to domain admin accounts, "just in case"**
- **Setting up new workstations with cloned images, all with the same local password**
- **Rotating administrator passwords only every 30-60 days**
- **Using an AD Group Policy to rotate one administrative password used for all machines**
- **Allowing accounts used by applications to have domain administrator privileges**

> **Because many existing implementations of Active Directory Domain Services have been operating for years at risk of credential theft, organizations should assume breach and consider the very real possibility that they may have an undetected compromise of domain or enterprise administrator credentials.**
>
> Microsoft, "Mitigating Pass-The-Hash and other Credential Theft, Version 2," 2014

Key finding:

Attackers used a Privileged Pathway to get to critical assets



Common practices that leave organizations wide open to pass-the-hash and similar techniques include

- **Permitting users to use accounts with administrative privileges on their own workstations**
- **Using the same administrator password for all local administrator accounts**
- **Not consistently enforcing password rotation or uniqueness policies for IT administrator accounts**
- **Setting up domain administrator accounts to be used to log into to domain controllers as well as servers and workstations**
- **Allowing administrator accounts to be used for day-to-day tasks such as checking email and browsing the Internet**

CYBER-Hygiene Program

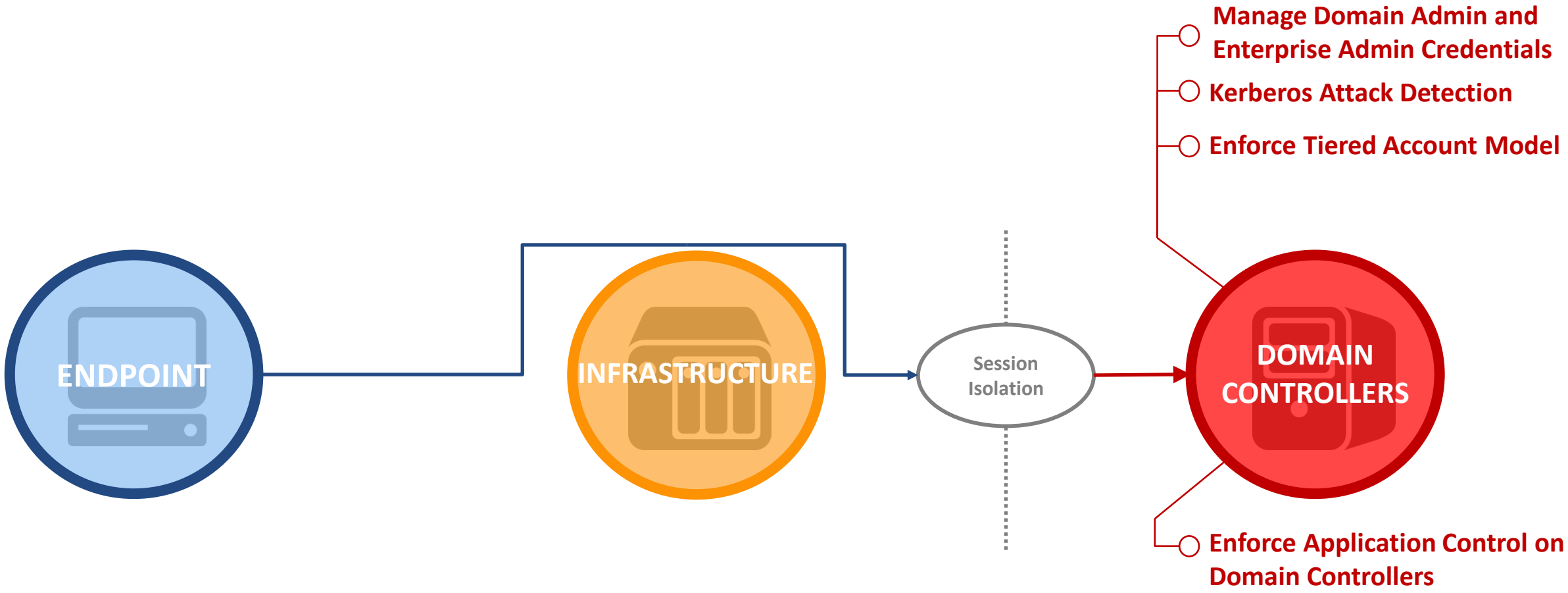
- Outlines the seven basic steps every PAS program should address over time
- Developed based on CyberArk's engagement with thousands of customers who embarked on PAS projects driven by:
  - Proactive project
  - Audit finding
  - Compliance requirement
  - Post-Breach remediation
- Focuses on steps that reduce the most risk relative to the level of resources and effort

15

PAS Hygiene Program Goals

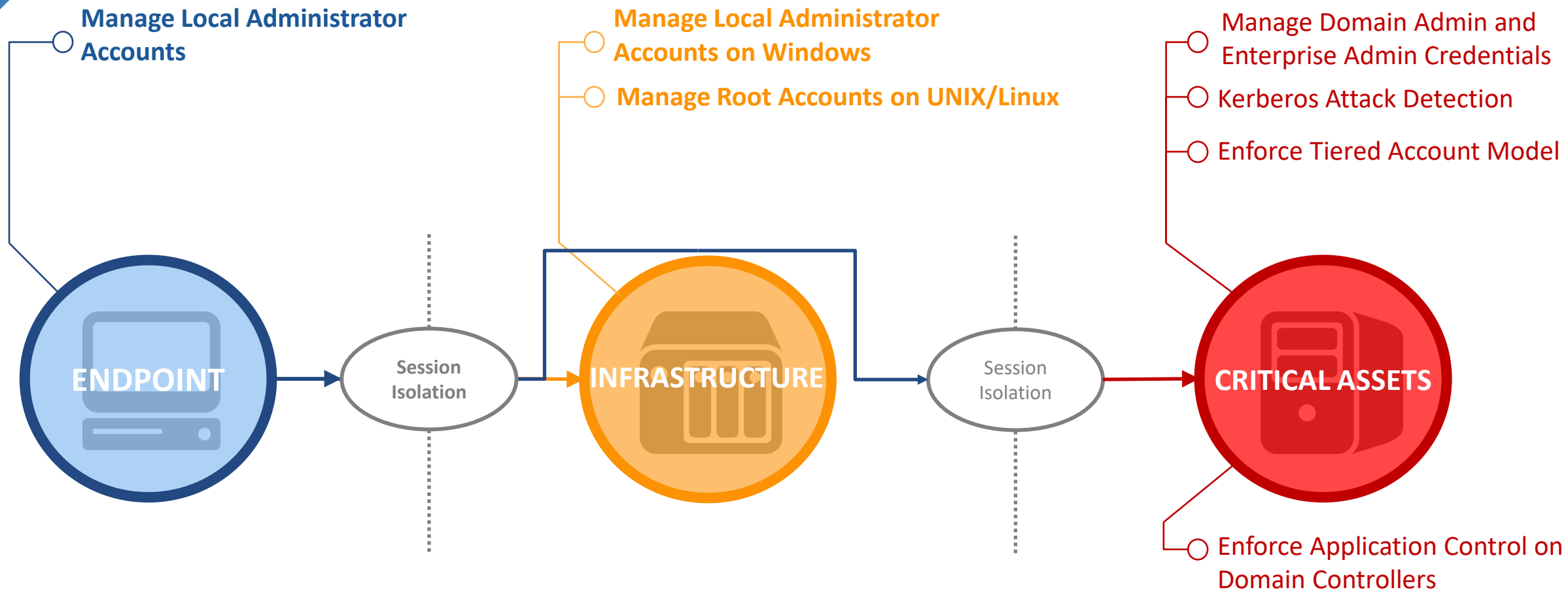
Step 1	Focus first on eliminating irreversible network takeover attacks (e.g., Kerberos Golden Ticket).
Step 2	Control & secure well-known infrastructure accounts.
Step 3	Limit lateral movement.
Step 4	Protect 3rd party privileged accounts.
Step 5	Manage SSH keys on critical Unix servers.
Step 6	Defend cloud & DevOps processes accounts.
Step 7	Secure shared IDs for business users (integrate and accelerate adoption of MFA).

1 Step 1: Irreversible Network Takeover Attacks



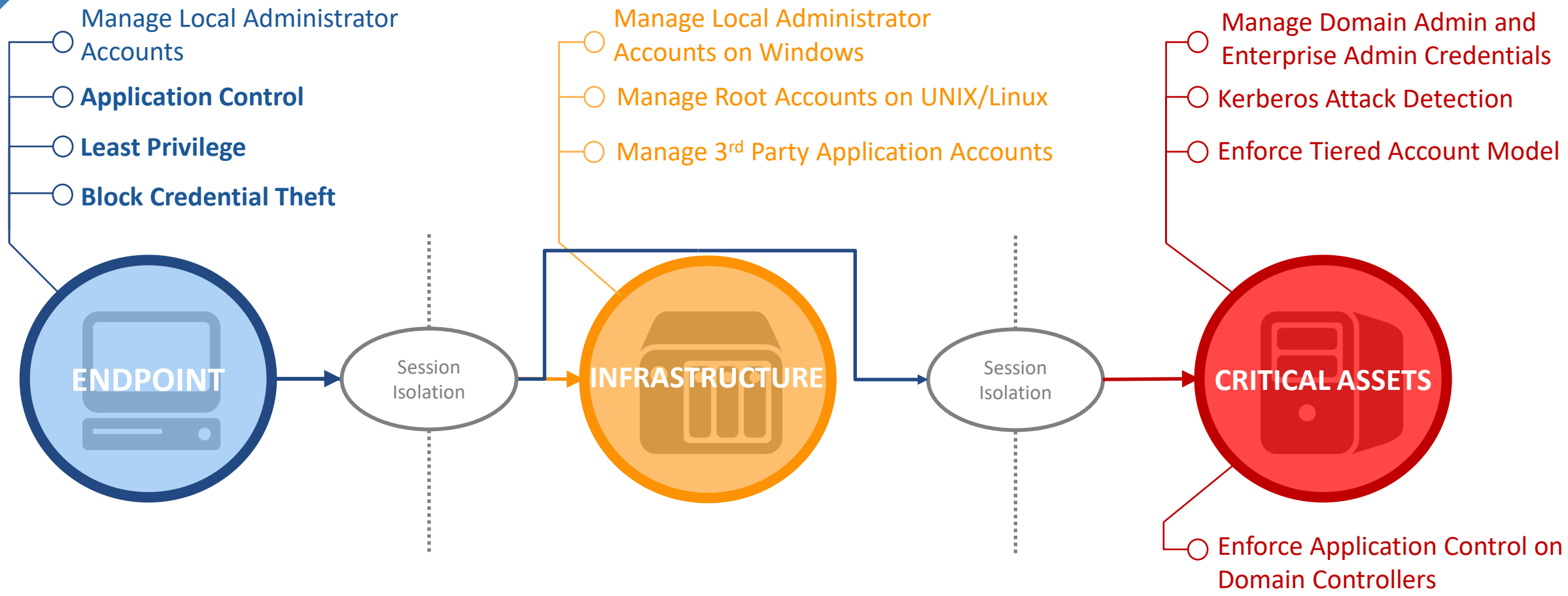
2

Step Two: Control & Secure Infrastructure and End Point Well-known Infrastructure Accounts

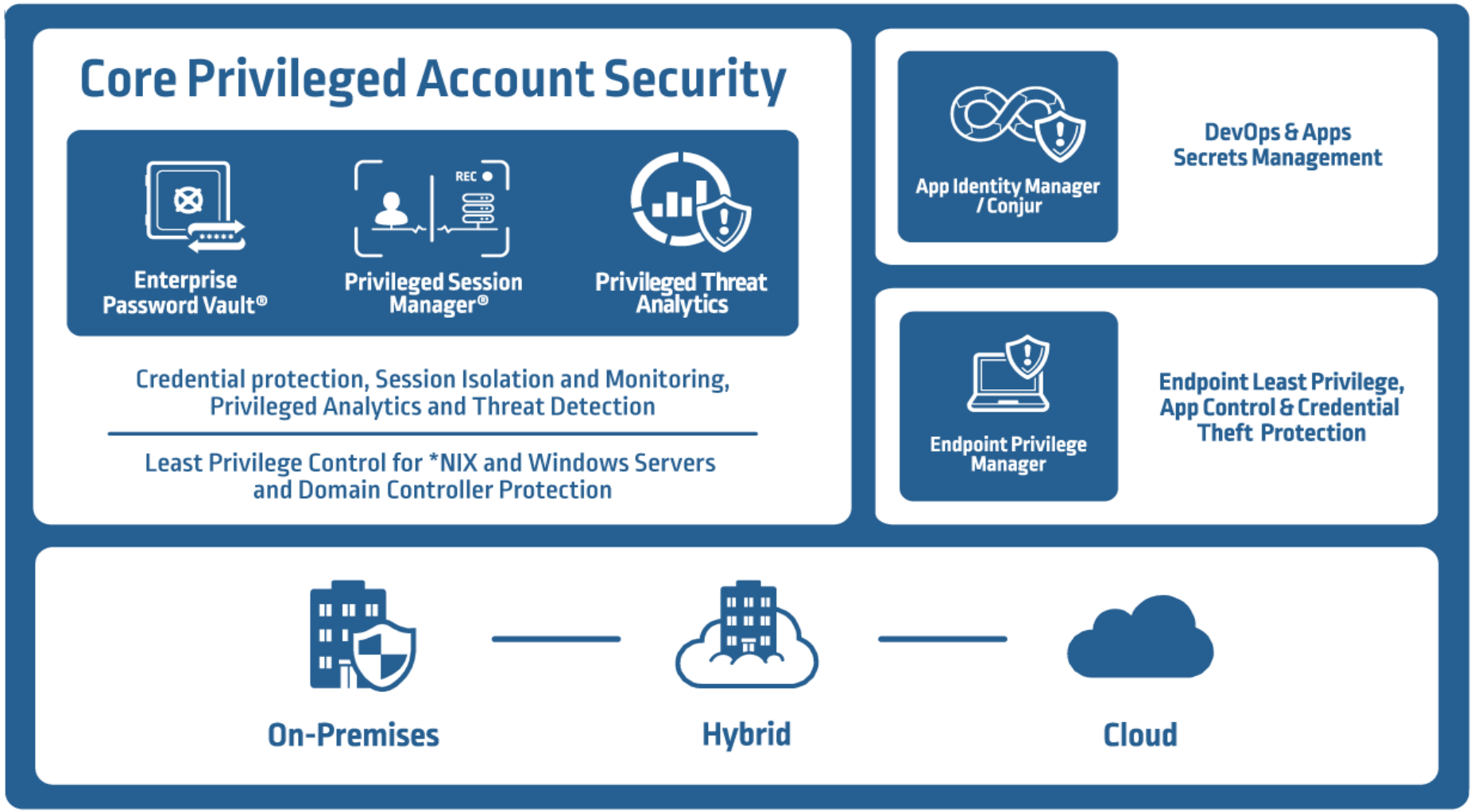


3

Step Three: Limit Lateral Movement



Questa è la visione CyberArk... venite al nostro stand



We have to think like the attacker

Look for exposed privileged accounts

- Exposed credentials alerts
- Unconstrained delegation alerts

Bypass Privileged Account Security controls

- Suspected credential theft
- Unmanaged privileged account

Known attacks for bypassing authentication

- Golden Ticket detection
- Overpass the Hash detection
- Hijacking Domain Accounts (DC Sync)

Go undetected while abusing privileged access

- Unusual access patterns
- Suspicious/risky privileged activity

Grazie!

Domande?

Alessio Pennasilico - apennasilico@clusit.it
Andrea Argentin – andrea.argentin@cyberark.com